EMA
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Sponsored by:

SECURITY JOURNEY

Secure Coding Practices – Growing Success or Zero-Day Epidemic?

January 2023 EMA Research Report

Christopher M. Steffen, CISSP, CISA, Managing Research Director and **Ken Buckler, CASP**, Research Analyst
Information Security, Risk and Compliance Management

Table of Contents

Introduction

From 2015 to 2021, the number of new vulnerabilities per year in the National Vulnerability Database grew from 6,487 to 20,139.* This increase in vulnerabilities may be due to a significant skills gap when it comes to secure software development. In 2019, a review of the top 20 computer science schools found that of the schools listed, only one had security as an undergraduate degree requirement for Computer Science.** Simply put, software developers are not being taught secure coding practices at colleges and universities, and with a significant number of organizations failing to invest in any secure coding training whatsoever, even some of the most seasoned developers in the industry may have little to no awareness of secure coding concepts.

With this alarming rate of increasing software vulnerabilities and the significant security skills gap for software developers across the workforce, how are organizations taking additional steps to ensure their applications are secure? We consistently hear about the cybersecurity skills gap in the news, but how has this issue affected software development?

EMA surveyed 129 professionals across multiple industry verticals, seeking to understand how organizations are tackling the difficult challenge of developing secure software applications. The results were quite eye-opening, revealing that over half of organizations performing software development struggle to fully integrate security into their software development lifecycle (SDLC). Many organizations are failing to make critical investments in enhancing the security knowledge of their development teams.

* CVSS Severity Distribution Over Time, https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time
** Cable, Jack, "Security requirements for computer science degrees." Aug 22, 2019. https://gist.github.com/cablej/f272747f2d545342aec7f34a1bfae4ef

Research Methodologies

EMA surveyed 129 professionals across over 20 different industry verticals. We found that 81.4% of respondents are focused on cloud-hosted application development, but only approximately 54% of respondents worked in industries requiring compliance with regulations, such as PCI, HIPAA, FISMA, etc.

We cross-analyzed survey data by industry, organization size, and involvement level of the respondent in the development process. For the most part, there were no statistical abnormalities or differences when analyzing the data in this manner. It appears that the successes and failures highlighted in this report are common across all industry verticals, as well as organization sizes.

At the end of this report, you will find an overview of the organization sizes and verticals, as well as the programming languages, frameworks, architecture, and development requirements in use by respondents.

Key Findings

SDLC

25% of organizations have adopted a “shift left” security SDLC model, and 5% are using a “legacy” security SDLC model.

69.3% of organizations have SDLCs that miss critical security steps. This includes 45.3% of organizations that do not have a dedicated validation step in their security SDLC, 20% of organizations that do not have a dedicated planning step, and 4% that do not have a dedicated implementation step.

89% of organizations adopting a “shift left” security SDLC model realized reductions in vulnerabilities, while only 25% of organizations utilizing “legacy” security SDLC realized reductions in vulnerabilities.

Code Security Strategy

95.3% of organizations utilize code reviews for secure coding, but only 87.6% train their employees on secure coding practices.

63.6% of organizations use in-house-developed training, while only 54.3% use third-party-developed training. Some organizations utilize a combination of third-party and in-house training.

68.1% of organizations not using third-party code realized great improvements in their code security, while only 45% of organizations using third-party code (open or closed source) saw similar improvements.

The Impact of Learning

100% of organizations using a combination of code reviews, code-scanning tools, and third-party training saw improvement in their code security.

Only 75% of organizations not using training saw improvement in their code security.

60.1% of organizations adopting continuous training realized great improvements in their code security, while only 3% did not see any improvement.

Voices of the Survey – Respondent Quotes and Feedback

Select Open-Ended Responses

Explain your organization's approach to securing custom-developed applications: what has worked, what hasn't worked, and where you believe your organization, or the industry, needs to improve.

[Our] applications are private by design since we are in a regulated industry. We strive for the minimum necessary in design and use of data. We utilize multiple security services and applications based on risk assessment and analysis and current and future threats.

Chief Compliance Officer,
Healthcare Industry

It all comes down to good coders on your team. If you can get the right people in there, then you should be ahead of any intrusions. **I think the industry just needs more development and learning at the base.**

IT Director,
Computer/Tech Services Industry

[Our approach is] rethinking security and integrating it into the development process. **The most common mistake in security is to treat it as a single step in the process, when security should be comprehensive and systematic.**

Development Director,
Computer/Tech Services Industry

What has worked: **Working with various third-party companies to manage proper code security practices**, performing regular security audits.

Where to improve: **We need to reduce reliance on third-party software libraries** in order to better own our own product.

C-Level Executive,
Finance Industry

Including **good security practices early in the software development process can avoid** costly refactoring or potentially **catastrophic security breaches later in the application's lifecycle**.

Executive IT Leader,
Computer/Tech Software Industry

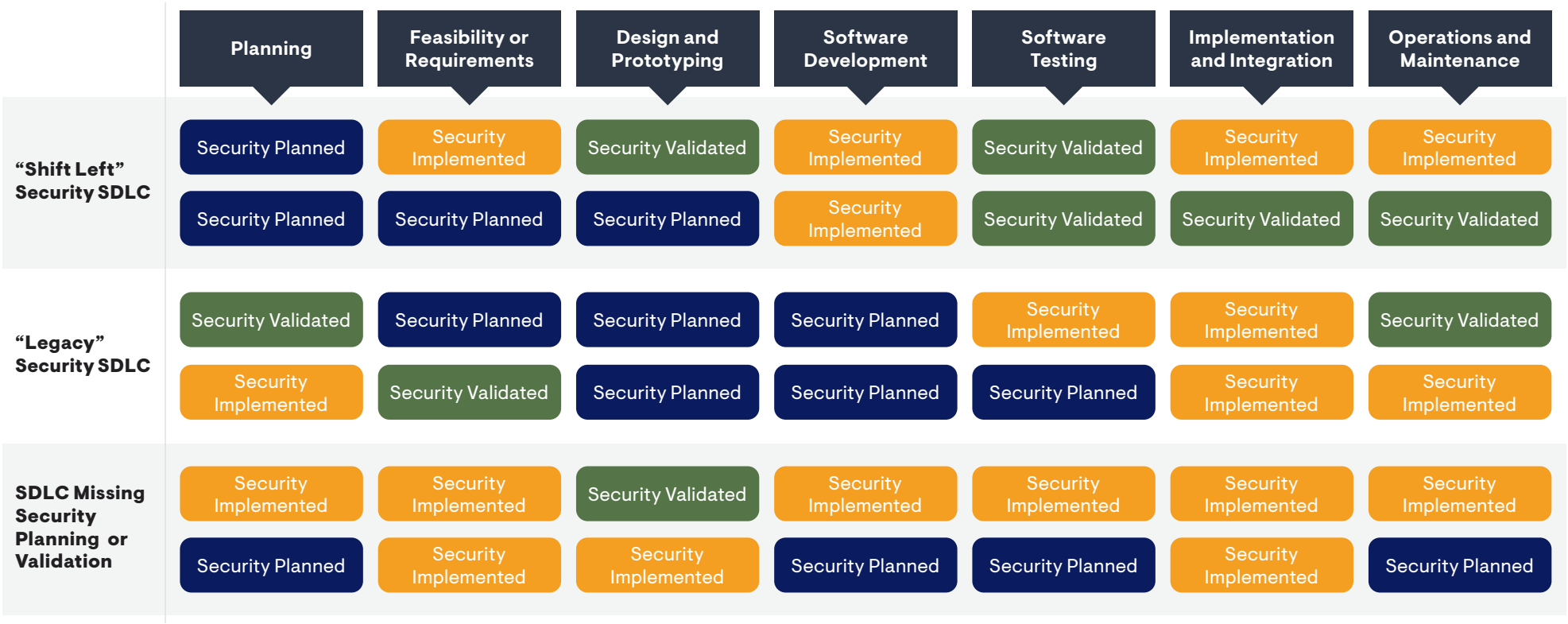
What has worked for us is taking more time to make sure that the applications are secure, and using a third-party vendor sometimes has really been a big help with security. **I do think that our organization needs to do more detailed training on application security.**

Executive IT Leader,
Retail Industry

Software Development Lifecycles

When analyzing software development lifecycles in use by organizations, several patterns emerged. Most "complete" security SDLCs, which included security planning, implementation, and validation, fit into "legacy" models in which security planning begins after software functionality has been planned and designed – or the more modern "shift left" model, in which security is planned and developed concurrently with software functionality.

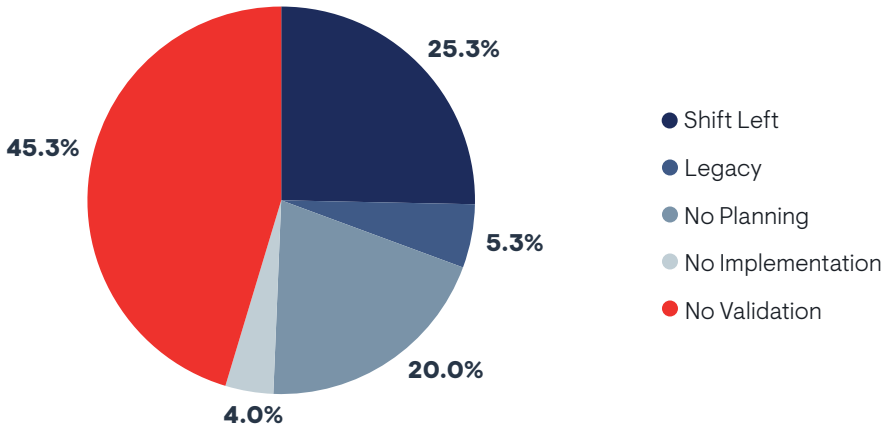
Some organizations clearly struggle with security in their SDLC, sometimes missing critical steps including planning, validation, and even implementation.



When looking at "complete" security SDLCs, "shift left" appears to be the most adopted strategy, but this only accounts for 25% of respondents.

Security appears to be a struggle for many organizations, with almost 70% of organizations missing critical security steps in their SDLC. Almost half of respondents stated that their organization does not dedicate a step in the SDLC for security validation. Another 20% of organizations don't plan their application security and instead rely heavily on implementation and validation. Some organizations, 4%, do not have a dedicated implementation step.

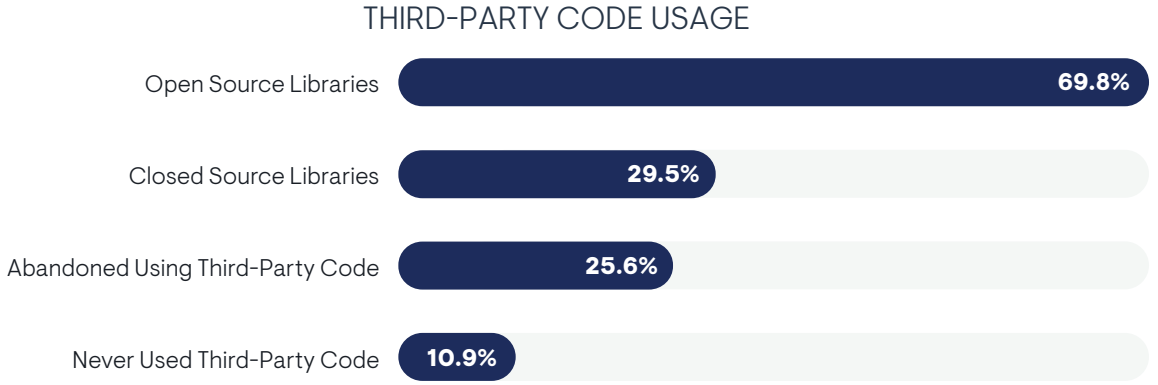
	Security Planned	Security Implemented	Security Validated
Planning	61.2%	25.6%	11.6%
Feasability or Requirements	43.4%	34.9%	16.3%
Design and Prototyping	30.2%	47.3%	20.2%
Software Development	31.8%	48.8%	18.6%
Software Testing	22.5%	41.9%	34.9%
Implementation and Integration	27.9%	44.2%	26.4%
Operations and Maintenance	30.2%	36.4%	31.0%



Secure Coding Practices

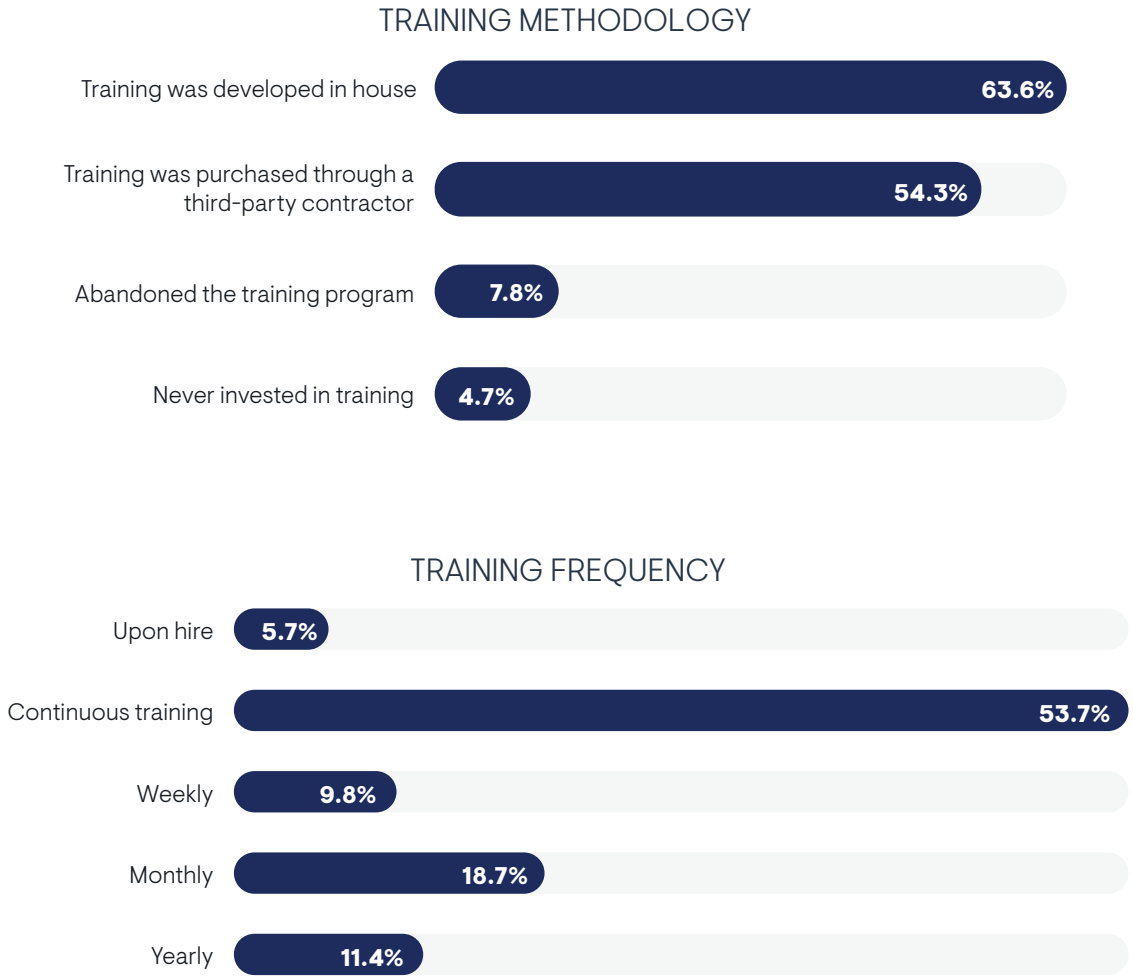
For this research, EMA looked at how often organizations utilize code reviews, code scanning tools, and secure code training. All three strategies did have a percentage of organizations that have abandoned their usage, with 2.3% of organizations abandoning code reviews, 6.2% abandoning code scanning tools, and 7.8% abandoning training programs. Across all three strategies, the most common reason for abandoning or never utilizing the strategies was concern over productivity impact.

We also looked at third-party code usage, finding that while many organizations utilize third-party libraries, 25.6% of organizations have abandoned third-party code, often due to security and regulatory compliance concerns.



Examining training methodology and frequency, we found that most organizations utilize continuous training that has been developed in house, or sometimes a combination of in-house and third-party training.

While productivity impacts were the most common reason for not investing in training, some other interesting reasons included the lack of training options available in the market, lack of understanding of the training, usage of black box security tests and vulnerability scans instead of training. Additionally, several confused respondents believe that their cloud service provider (CSP) protects their applications from attacks and that no additional security investment is needed. Unfortunately, CSPs provide no protection for cloud application vulnerabilities as part of the shared responsibility model.



Measuring Results

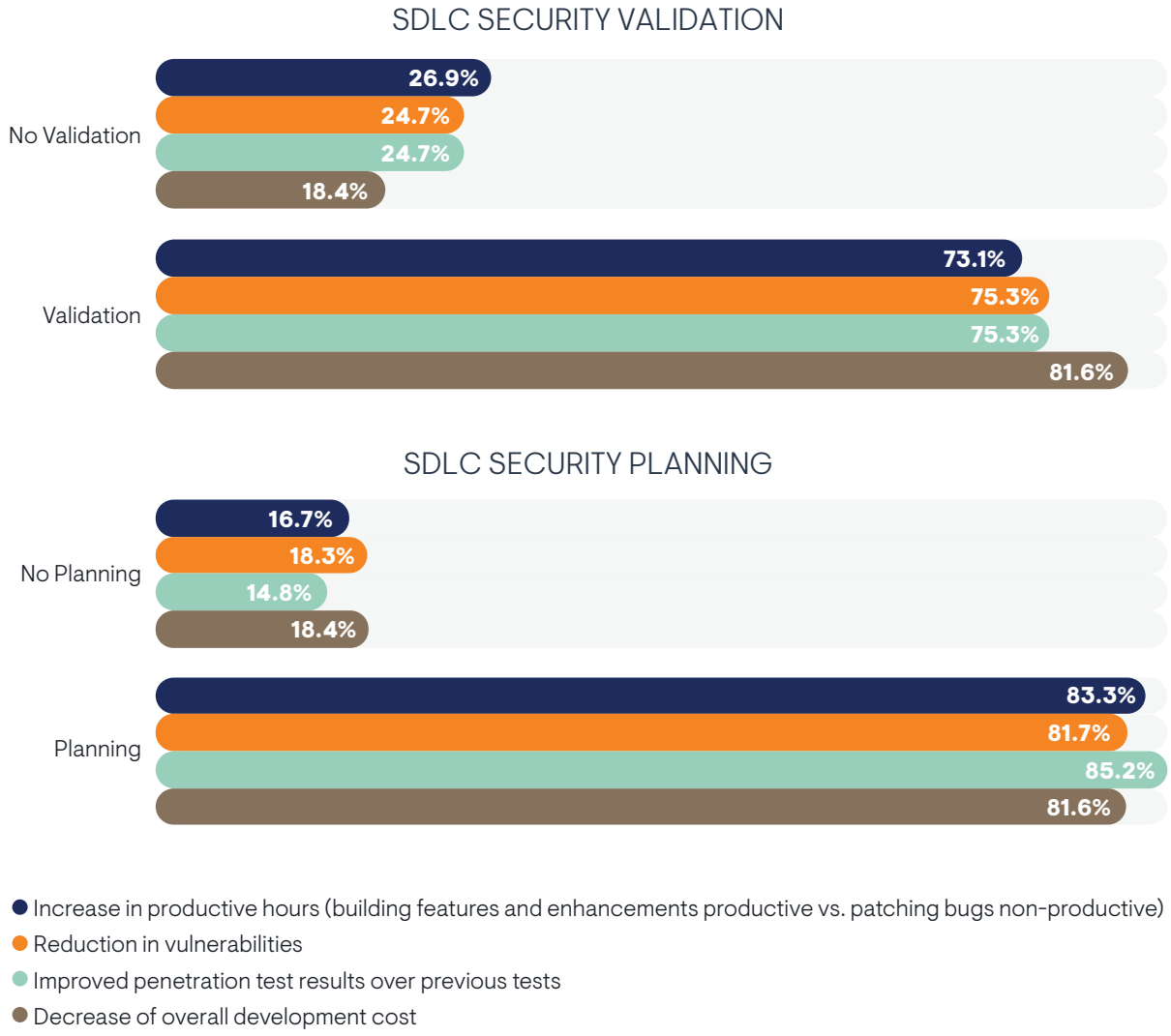
SDLC

Given the significant number of organizations not using planning or validation in their SDLC, we felt it was important to analyze the security and productivity impacts of these trends.

The results speak for themselves and stress the importance of integrating security planning and validation into the SDLC.

Organizations without security validation or planning in their SDLC are significantly hindering their ability to reduce vulnerabilities and improve productivity.

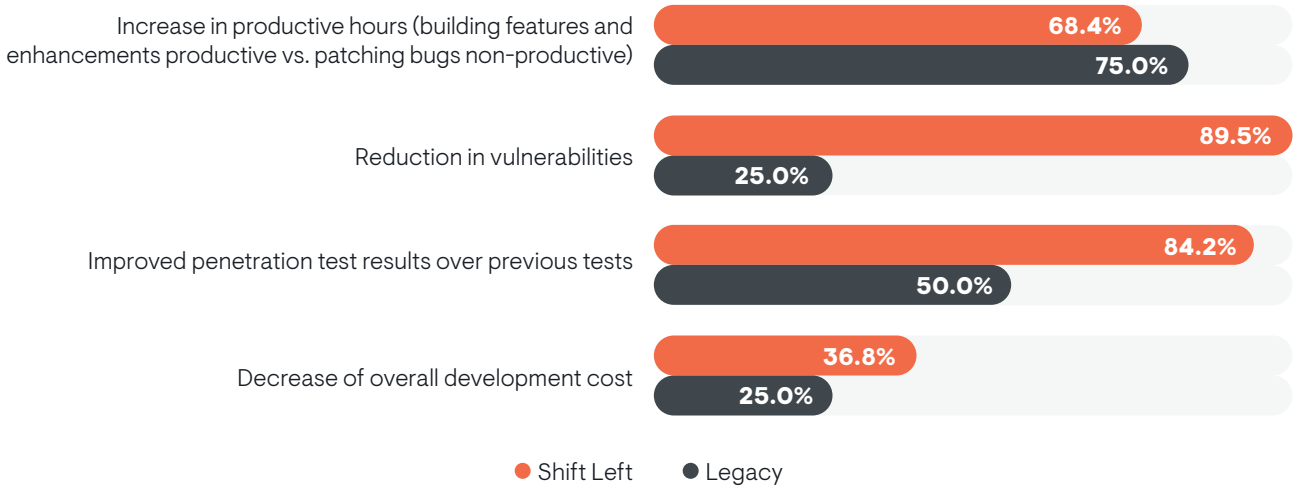
With almost 70% of organizations missing at least one critical step in their SDLC, it's important that these organizations adjust their strategy immediately.



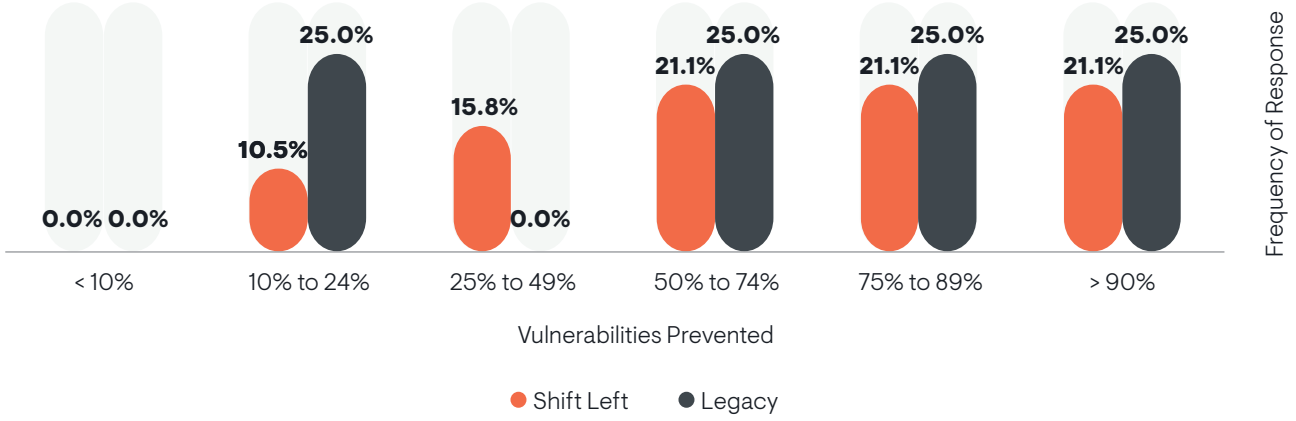
When examining SDLC strategies, "legacy" SDLC often provided more productive hours for developers than "shift left." However, this productivity improvement comes at a cost – both in security costs and overall development costs. Legacy security SDLC provides the illusion of more productive hours, but at the cost of spending more hours later fixing vulnerabilities.

While at first glance "legacy" appears to prevent more vulnerabilities from reaching production, this chart is misleading. There is a 1-in-4 chance that under the "legacy" model, fewer than 25% of vulnerabilities will be prevented from reaching production. This is undoubtedly because in the "legacy" model, security implementation only occurs after initial development of functionality is completed.

SDLC SHIFT LEFT VS. LEGACY



SDLC AND CODE SECURITY VULNERABILITY PREVENTION

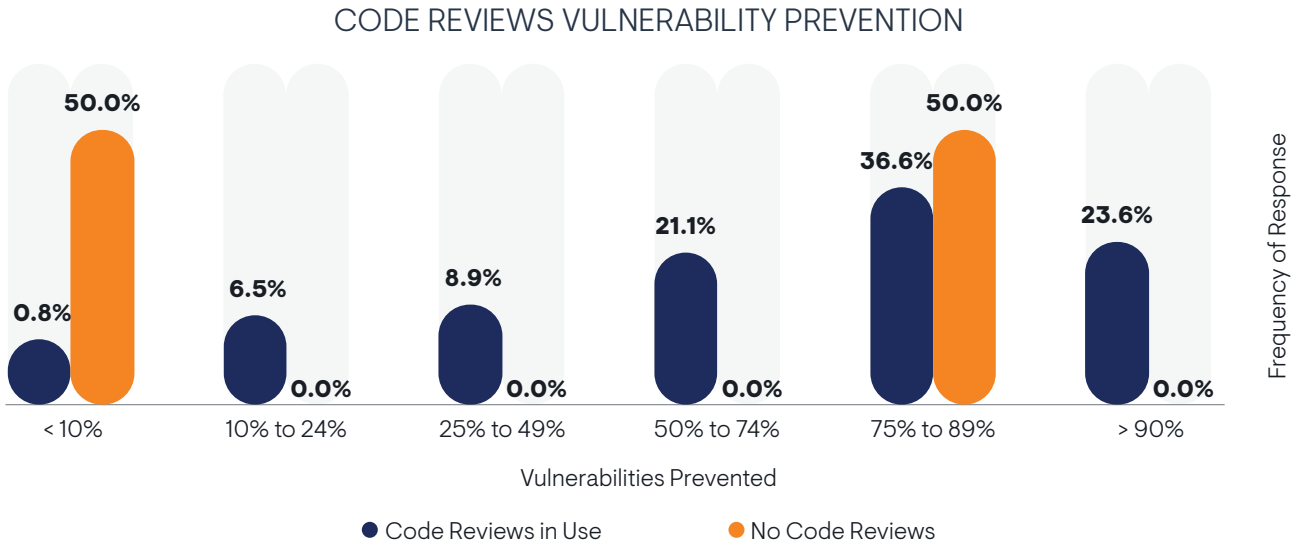


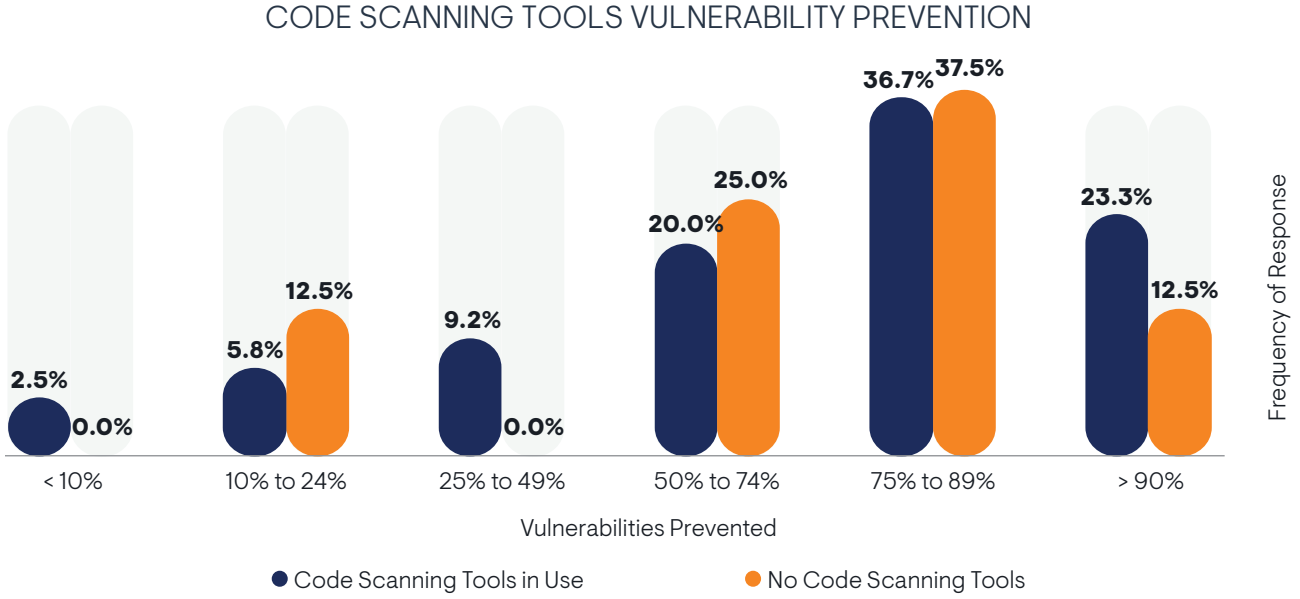
Secure Coding

The two most commonly used code security methods – code reviews and scanning tools – provide some interesting data when analyzing their effectiveness.

Code reviews appear to be very hit or miss, with 50% of organizations that don't conduct code reviews outperforming 75% of those that do. Undoubtedly, this has more to do with the skill of the reviewers and less to do with the review process itself.

Code scanning tools only provide a minimal advantage over not using tools. Overall, only 10% of organizations prevented a higher percentage of vulnerabilities than organizations not using code scanning tools. Code scanning tools are often very expensive, and this raises the question: are organizations truly getting the value they should from these tools?

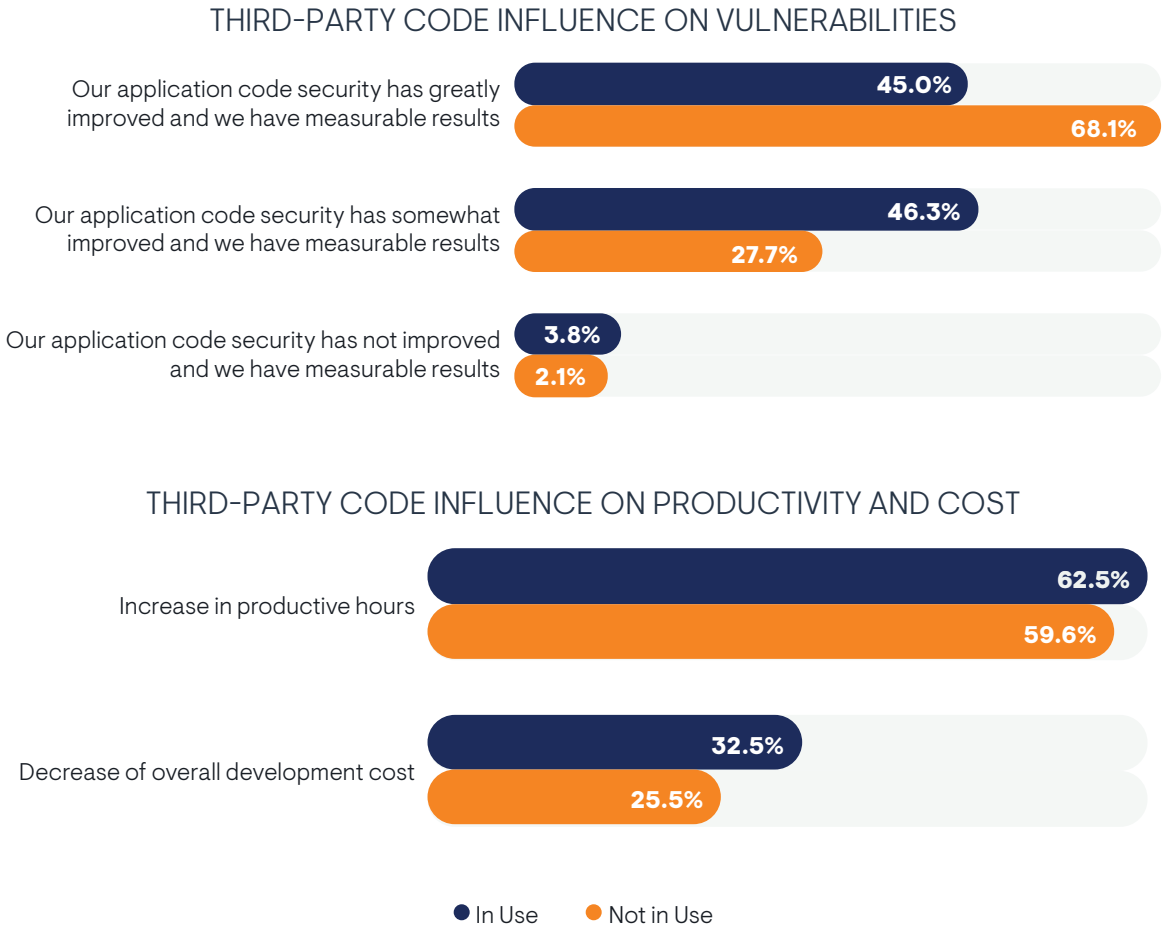




Third-Party Code

The usage of third-party code appears to present an interesting tradeoff. Organizations that do not use third-party code appear to see great improvements in their code security, but at a slight productivity and application development cost impact.

This tradeoff seems to be a prevalent struggle organizations face when it comes to code security. Developing secure software requires some sacrifice because organizations must invest in tools or time for software to be truly secure. While third-party libraries provide a "shortcut" for development timelines, additional investment is then required to ensure those third-party libraries are properly vetted, then securely implemented.

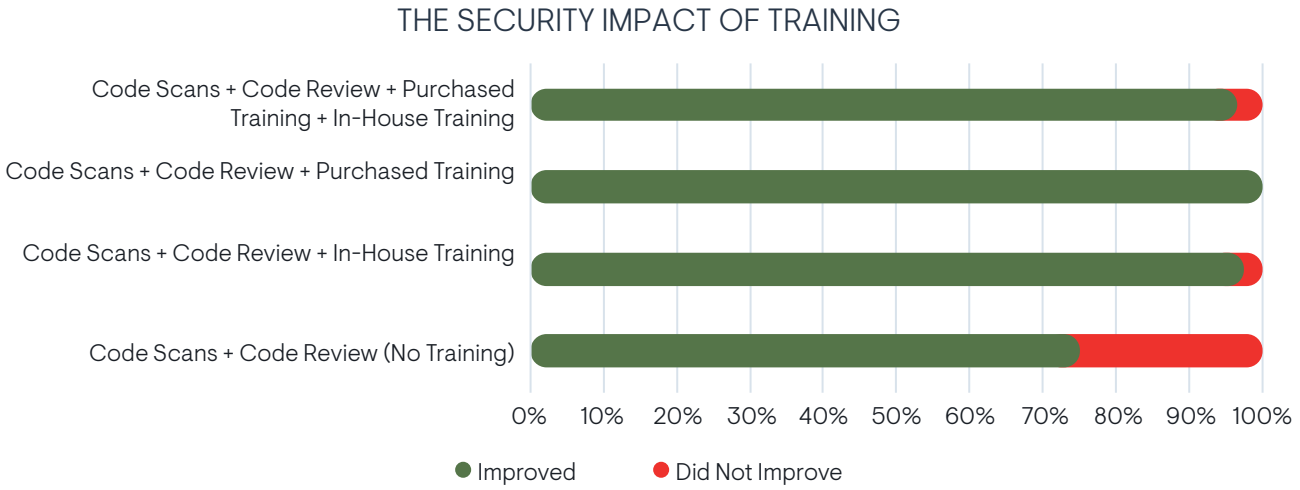


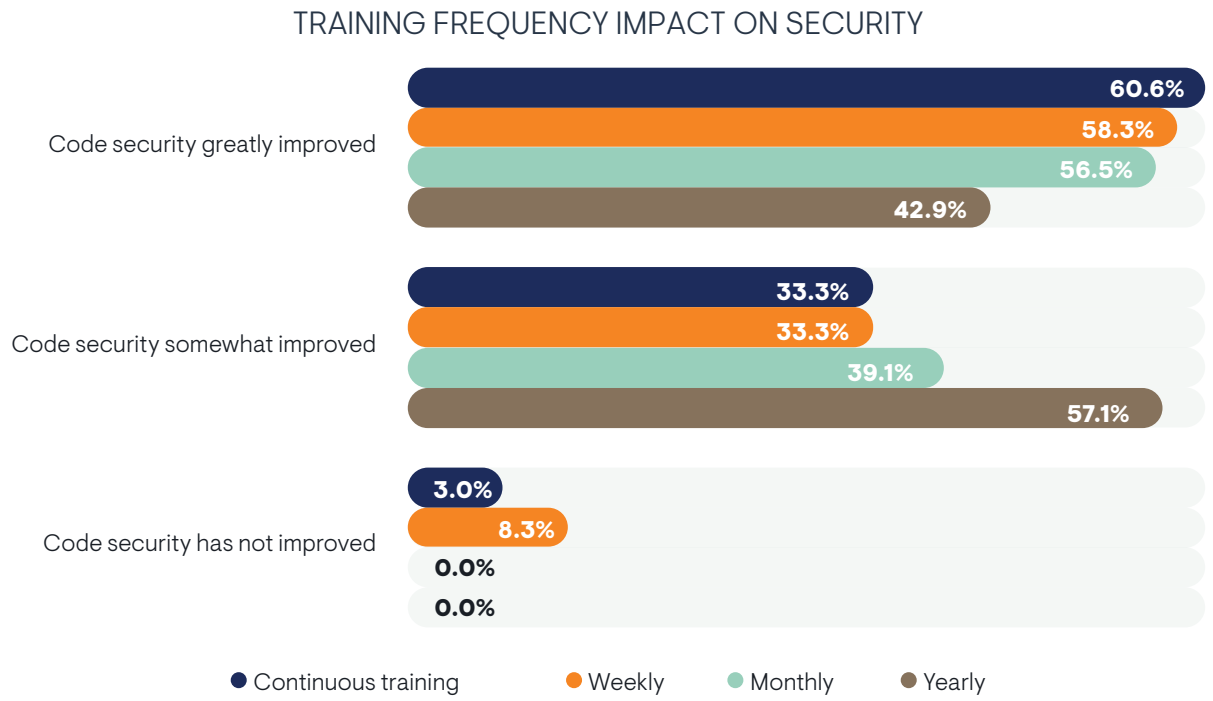
Training

When it comes to improving code security, training seems to be an underutilized method with high return on investment. Organizations that don't have training only see a 75% improvement in their security, versus over 96% if they utilize training.

While third-party-developed training (100% improvement) provides a slight competitive edge over in-house training (97.4% improvement), developing and maintaining training in-house can be expensive, requiring an entire team with very specialized skillsets to keep training up to date. Clearly, third-party training provides a more realistic option and better return on investment.

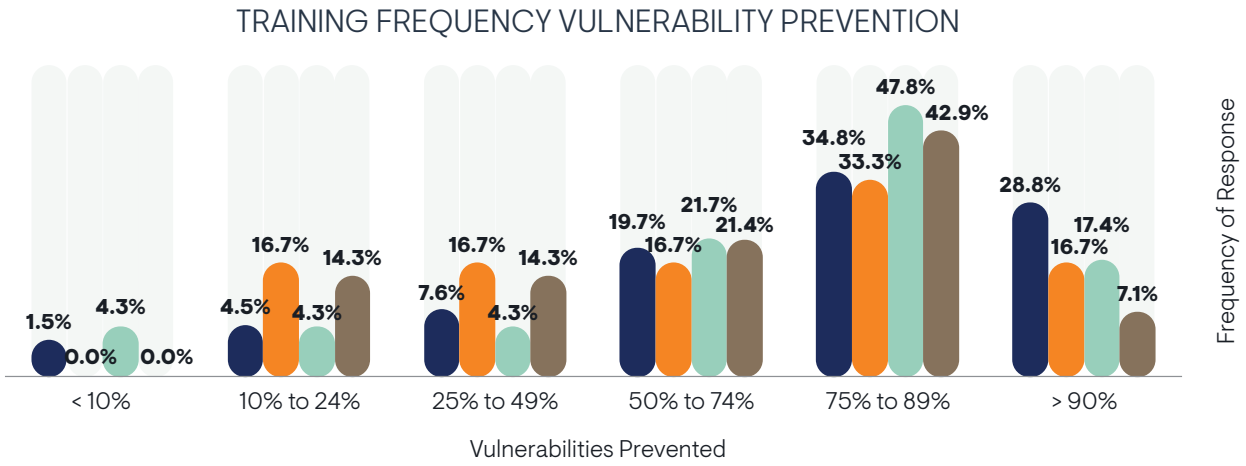
Frequency of training also appears to play a role in improving code security. The more often employees are trained in secure coding practices, the more often their code security greatly improves.

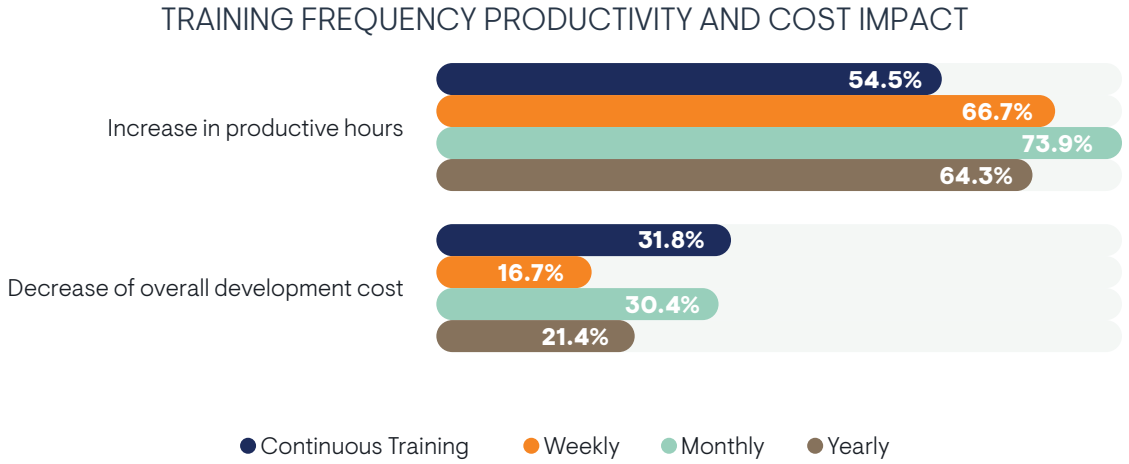




When examining training frequency vs. vulnerabilities prevented, continuous training is the clear winner, with 28.8% of respondents utilizing continuous training preventing over 90% of vulnerabilities from reaching production. Another 33.3% of respondents stated that between 75% and 89% of vulnerabilities were prevented from reaching production with continuous training.

While continuous training did not experience as high of an improvement in productive hours as other strategies, long-term usage of continuous training was the leading strategy for decreasing development cost. This is likely due to developers spending less time after initial development fixing security vulnerabilities.





EMA Perspective

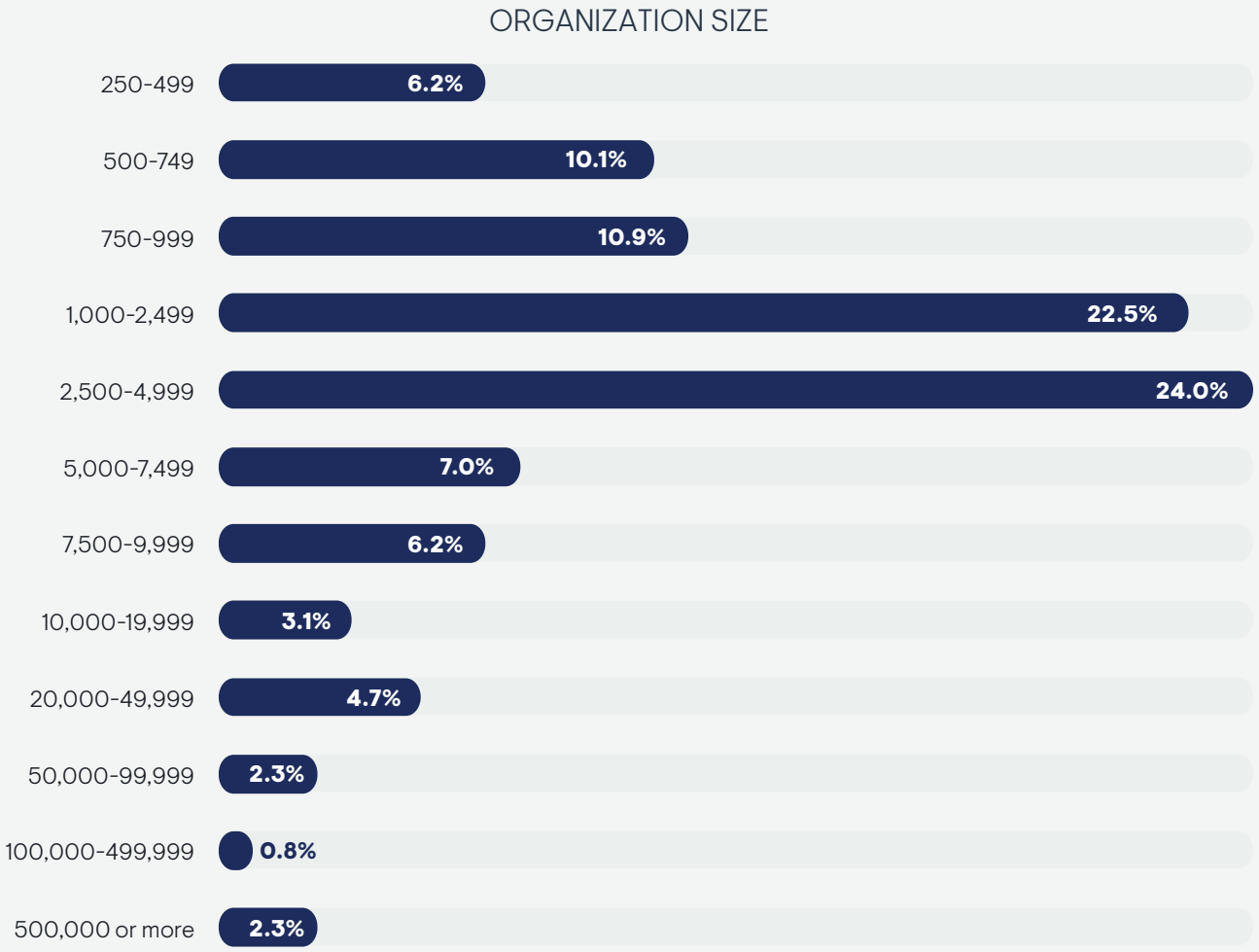
After reviewing the data, EMA believes the best approach to secure software development is a combination of code reviews, code scanning tools, and a stronger emphasis on continuous, third-party training. Significantly important is adopting a full security SDLC including planning, implementation, and validation. While a "shift left" approach does appear to be more effective, even adopting a legacy security model would be preferable to the incomplete security SDLCs used by almost 70% of organizations today.

All too often when it comes to cybersecurity, the human element is the most overlooked component of any system. With lowest adoption rates (54%) and highest code security improvement rates (100%), third-party training appears to be the critical component in which some organizations are failing to invest. Code reviews without training may ultimately prove to be futile efforts, simply checking a compliance checklist box that the code was reviewed. After all, how can those reviewing the code understand whether the code is secure if those reviewers haven't been given the proper training in the first place?

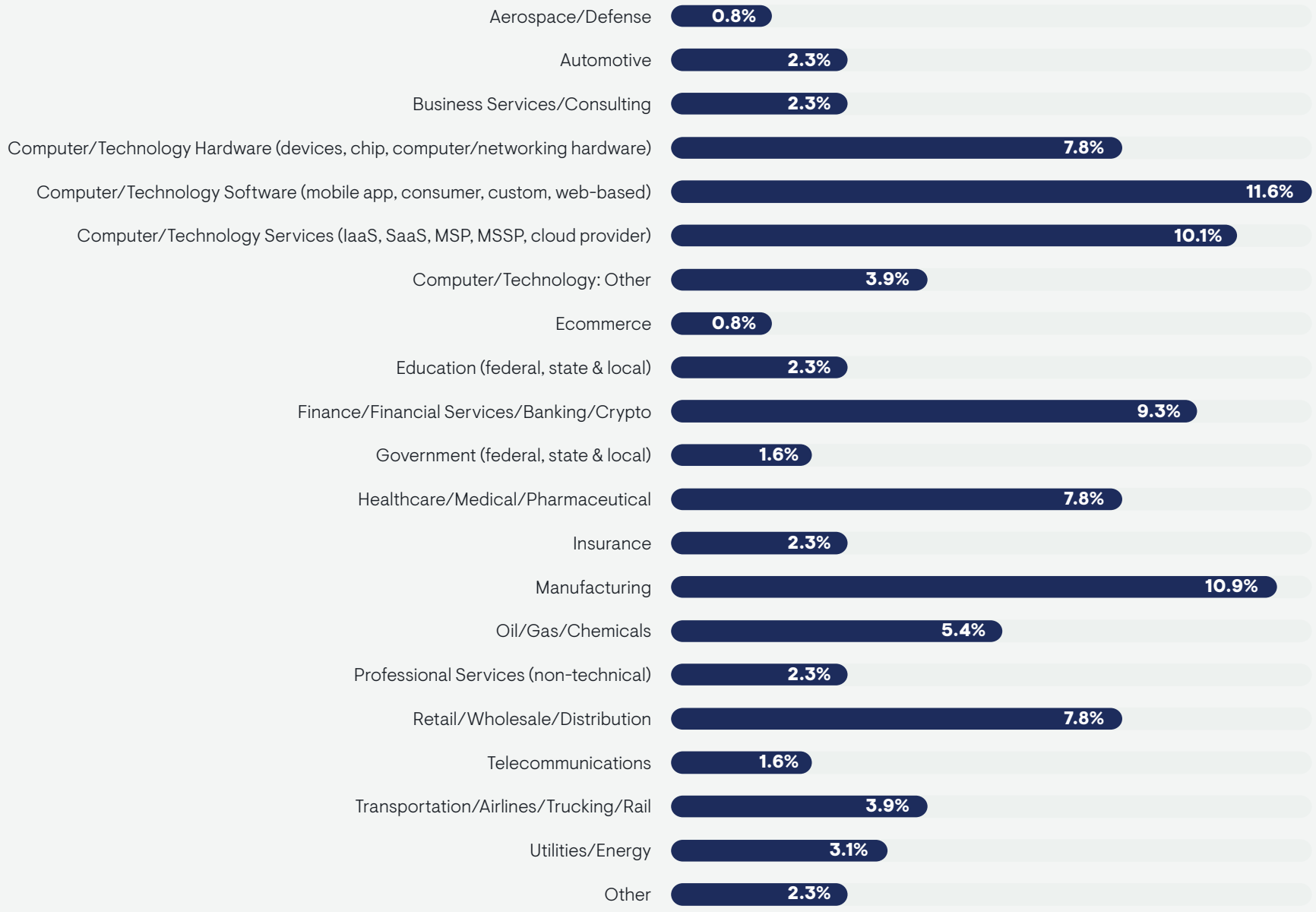
Code scanning tools have their place, but they simply don't have the discernment to catch everything. It's much better for developers to write secure code initially than hope that a code scanning tool will catch the vulnerability before it makes it to production – especially when only 10% of organizations utilizing code scanning tools prevented more vulnerabilities than those who don't. Code scanning tools should only supplement secure coding efforts and not be the critical wheel in the system, especially when almost 70% of organizations are struggling with even basic security SDLCs. Tools simply cannot fix broken security practices.

Across all industry verticals, software development must shift its focus away from heavily relying on code scanning tools and more on people and processes. The consequences for failing to correct this approach to secure coding are far-reaching, beyond even the organizations developing the software and affecting every user of these vulnerable applications.

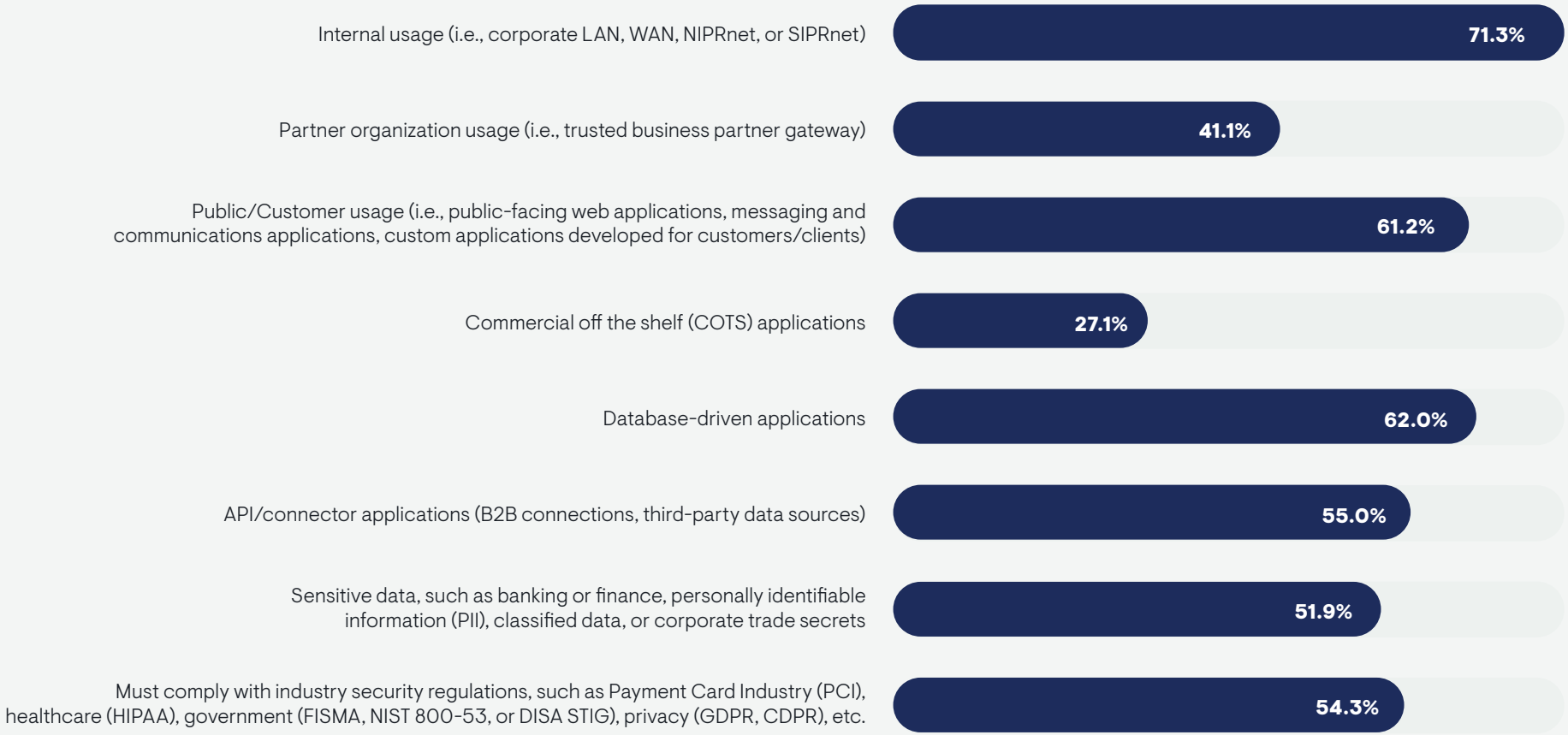
Demographics


ORGANIZATION SIZE
250-499
6.2%
500-749
10.1%
750-999
10.9%
1,000-2,499
22.5%
2,500-4,999
24.0%
5,000-7,499
7.0%
7,500-9,999
6.2%
10,000-19,999
3.1%
20,000-49,999
4.7%
50,000-99,999
2.3%
100,000-499,999
0.8%
500,000 or more
2.3%

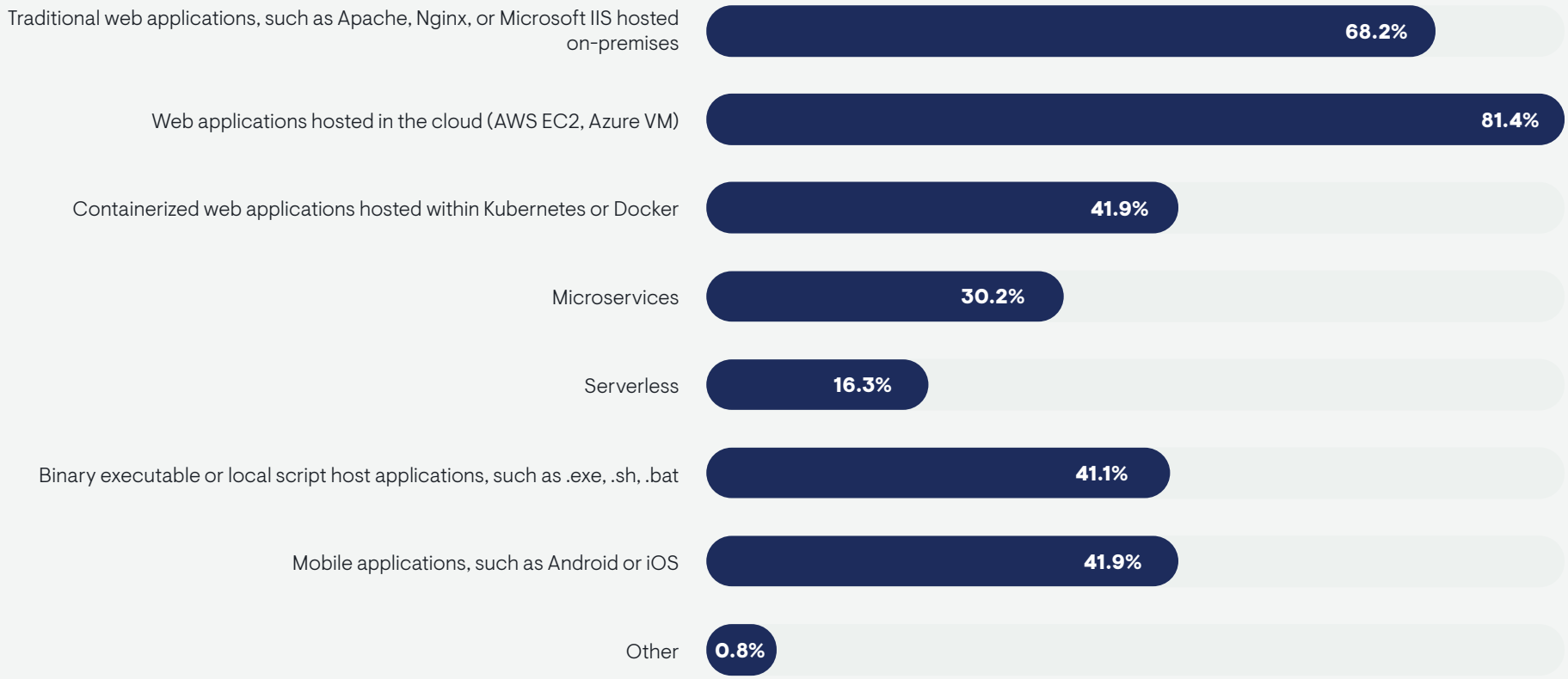
PRIMARY INDUSTRY



SOFTWARE DEVELOPMENT REQUIREMENTS



APPLICATION ARCHITECTURE



LANGUAGES AND FRAMEWORKS

Security Journey

Security Journey helps enterprises reduce vulnerabilities with application security education for developers and everyone in the SDLC.

Two application security training companies became one in the spring of 2022 when HackEDU acquired Security Journey and adopted the Security Journey name. Today, Security Journey offers robust application security education tools to help developers and the entire SDLC team recognize and understand vulnerabilities and threats and proactively mitigate these risks.

Foundational knowledge for all. Hands-on, skills-based sandboxes for developers. One path to build a security-first culture.

Start your journey to safer apps at https://www.securityjourney.com/

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com. You can also follow EMA on Twitter or LinkedIn.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 www.enterprisemanagement.com

4237.011123